Қазақстан Республикасы Тәуелсіздігінің 30 жылдығына арналған «Сейфуллин оқулары – 17: «Қазіргі аграрлық ғылым: цифрлық трансформация» атты халықаралық ғылыми – тәжірибелік конференцияға материалдар = Материалы международной научно – теоретической конференции «Сейфуллинские чтения – 17: «Современная аграрная наука: цифровая трансформация», посвященной 30 – летию Независимости Республики Казахстан.- 2021.- Т.1, Ч.3 - С.44 - 46

СРАВНЕНИЕ ПРОТОКОЛОВ IPV4 И IPV6 ДЛЯ ОБЕСПЕЧЕНИЕ СЕТЕВОЙ БЕЗОПАСНОСТИ

Нуртазаев М.О., Хамзина Б.Е.,
Мугазов А.Т.

В данной статье представлен сравнительный анализ угроз сети для протоколов IPv4 IPv6. Автор анализирует безопасность сетей, сильные и слабые стороны устойчивости протоколов. Рассмотрены типы вирусных атак, существующие для протоколов, и актуальные угрозы для сетей IPv6.

Ключевые слова: протокол, IPv6, IPv4, угроза, безопасность, сеть.

Современная IP сеть всегда требует улучшения общей функциональности, а также некоторых специфических функций безопасности, в случае их необходимости. Для успешного решения проблем, связанных с безопасностью, необходимо принятие и применение протоколов. На сегодняшний день доминирующим эталонным стандартом Интернет-протокола является IPv4, имеющий ограниченное пространство IP-адресов, а также недостаточную безопасность. Так как IPv4 определяет 32-битное пространство и поле IP-адреса, то доступное адресное пространство, имеющееся для подключения пользователей стремительно заканчиваются. В протоколе IPv4 предоставлена единственная функция безопасности, которая позволяет пользователям отправлять сведения о защищенности и обработке данных. Понимая об ограничениях имеющихся в инфраструктуре Интернета, основанной на наборе протоколов IPv4, сетевая рабочая группа Инженерной группы Интернета (IETF) рекомендовала новый набор протоколов, названный IPv6 [1]. С целью исследования потенциальных путей решения сетевой безопасности, нами выявлены и определены различия между протоколами IPv4 и IPv6.

Главной различием позволяющей новой версии протокола быть востребованной, это увеличение адресного пространства при ее использовании. Если адресное пространство протокола IPv4 позволяет использовать только 32-битный IP-адрес, то IPv6 дает возможность использовать 128-битный IP-адрес. С увеличенным размером IP-адреса можно определить вплоть до 2128 или 3,4 х 1038 различных IP-адресов, т.е многоадресная рассылка адресована более широкому использованию эффективных коммуникаций "один ко многим". Anycast, как метод рассылки пакетов, адресует избыточные службы, используя не уникальные адреса.

С появлением протокола IPv6, используется новый тип структуры протокола, в котором изменению подвергается структура протокола,

называемая заголовок. Измененный заголовок IPv6 позволяет использовать другой тип структуры, позволяющий протоколу работать более качественно. Заголовок IPv6 всегда содержит в заголовке пакета 40 байт и 8 полей. В отличие от заголовка IPv4, заголовок IPv6 не может различаться по размеру. Поле контрольной суммы не используется в IPv4, а протокол IPv6 не использует контрольные суммы заголовков, т.к. контрольная сумма уровня канала всего пакета, предусмотренная в протоколах, таких как PPP и Ethernet, в сочетании с использованием контрольных сумм в протоколах верхнего уровня, таких как TCP и UDP, является достаточной. Таким образом, маршрутизаторы, использующие IPv6, освобождаются от задачи пересчета контрольной суммы всякий раз, когда пакет изменяется, например, за счет уменьшения счетчика ограничения переходов на каждом переходе. [1] Поля фрагмента, которые появляются в заголовке IPv4, удалены из основного заголовка IPv6. Информация о фрагменте перенесена в заголовок расширения [1].

Изменяя структуру протокола, рассмотрим протоколы защиты и безопасности IPv6, которые используются в безопасности протокола IP. (Рисунок)

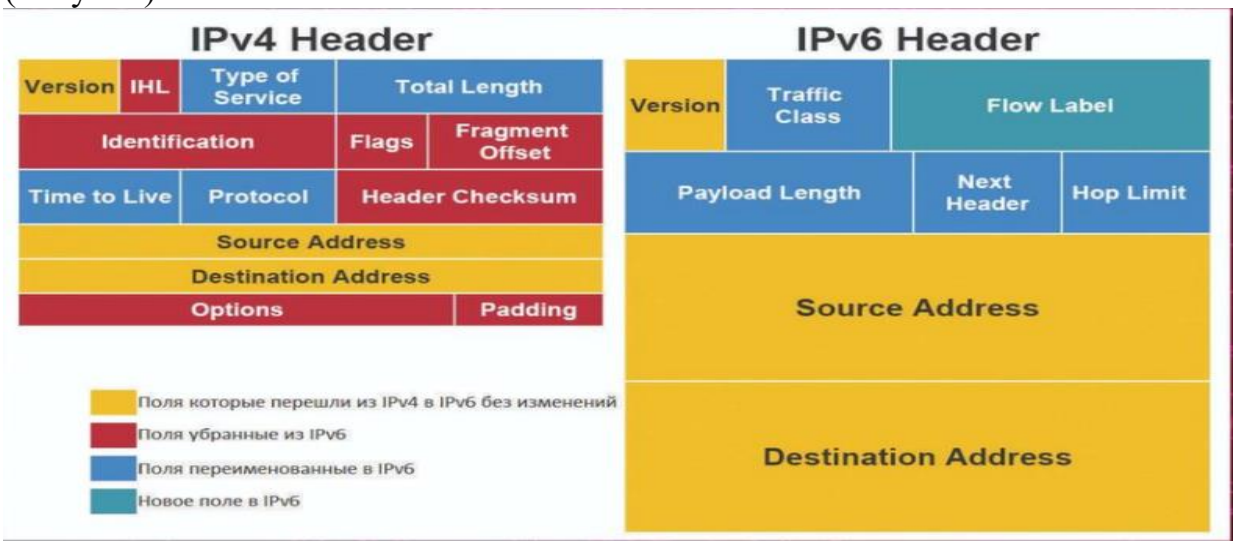

Рисунок. Содержание заголовков

Термин IPsec относится к набору протоколов от IETF, обеспечивающих шифрование сетевого уровня и аутентификацию для сетей на основе IP. Целью IPsec является аутентификация или шифрование всего трафика на уровне IP. Хотя IPSec доступен для реализаций IPv4, протокол может работать и без протокола IPsec, но используя сети IPv4 и IPv6 протокол IPsec является обязательным для предотвращения большого объема угроз. Поддержка IPSec в реализациях IPv6 — это требование, которое обязательно должно быть учтено. IPsec является обязательным в протоколе IPV6 и IPV4. В IPv4 широко используются NAT, который позволяет увеличивать пространство, но и подвергать пользователей устройств опасности, но IPv6 расширяет адресное пространство и делает NAT ненужным. IPv6 увеличивает использование IPsec в сквозной связи. В IPv6 протокол IPSec реализуется с использованием заголовка аутентификации и заголовка расширения инкапсуляции полезной нагрузки безопасности. Кроме того, поскольку большинство нарушений безопасности происходит на уровне приложений, даже успешное развертывание IPsec с IPv6

не гарантирует какой-либо абсолютной безопасности для существующих атак кроме возможности определить источник атаки.

Т.к безопасность с помощью протоколов, не гарантирует полного контроля за системой, и поэтому стоит рассмотреть нам типы вирусных атак, которые создают новые угрозы безопасности в сетях. Примером атаки, которая происходит как в сети IPv4, так и сети IPv6, является атака с перехватом. Атака сниффинга включает перехват данных, передаваемых по сети. Если конфиденциальные данные передаются по протоколу с открытым текстом, они могут быть легко скомпрометированы злоумышленником, запустившим сниффинговую атаку. Тип атаки сниффинга можно избежать за счет правильного использования архитектуры безопасности IPsec, которая используется в IPv4 как опция, и в IPv6 как обязательная.

При рассмотрении атаки типа sniffing, исследование угроз переходит на новый уровень. Данный этап угрозы безопасности затрагивает проблемы с безопасностью уровня приложений в эталонной модели OSI [2]. Угрозы на уровне приложений сегодня являются наиболее часто используемыми злоумышленниками, такие как переполнение буфера, атаки веб-приложений, различные типы вирусов и червей. Переход на протокол IPv6 не предотвратит компьютерные системы и сети от этих атак и не предотвратит их последствия, поскольку и IPv4, и IPv6 являются протоколами сетевого уровня, и эти типы атак происходят на прикладном уровне сетевой модели OSI.

Рассматривая атаки, возникающие в сетях, большую угрозу занимает лавинообразная атака. Данная атака обозначает переполнение сетевых устройств таких как коммутаторы, маршрутизаторы или пользователей, большим объемом сетевого трафика. Целевое устройство не может обрабатывать такой большой объем сетевого трафика и становится недоступным или не обслуживается. Атака лавинной рассылки может быть локальной или распределенной атакой типа «отказ в обслуживании», когда целевое сетевое устройство наводняется сетевым трафиком со многих хостов одновременно. Этот тип атаки также может повлиять на сети IPv6, поскольку основные принципы атаки, лавинообразной остаются неизменными. Новые типы заголовков расширений в IPv6, новые типы сообщений ICMPv6 и зависимость от многоадресных адресов в IPv6 могут обеспечить новые способы неправильного использования при хакерских атаках лавинообразной атаки.

Таким образом, переход от протокола IPv4 к протоколу IPv6 является долгим процессом, поскольку оба протокола будут существовать вместе и переход будет постепенным. Для обеспечения плавного перехода на новую версию протокола разработаны различные механизмы перехода. Важными из них являются туннелирование и конфигурации с двумя стеками.

Данный переход может привести к появлению новых, ранее неизвестных угроз безопасности, поэтому важно рассмотреть возникающую угрозу, которая присуща для протоколов ICMPv6. В сетях IPv4 существует возможность заблокировать большинство сообщений ICMP без прямого влияния на функциональную работу сети. Блокировка сообщений ICMP использовалась на постоянной основе для повышения безопасности в сетях IPv4. С другой стороны, в сетях IPv6 важные механизмы такие как обнаружение соседей и

механизмы обнаружения максимального блока передачи пути, зависят от некоторых типов сообщений ICMPv6. Следовательно некоторые сообщения ICMPv6 проходят проверку на разрешения из-за правильной работы сети. Спецификация ICMPv6 также позволяет отправлять ответ об ошибке на многоадресные адреса. Этим фактом злоумышленником может воспользоваться. Отправив подходящий пакет на адрес многоадресной рассылки, злоумышленник может вызвать несколько ответов многоадресного пакета, который будет нацелен на жертву [3].

В ближайшем будущем протокол, IPv6 заменит протокол IPv4. Новый набор протоколов предоставляет на данный момент большое количество преимуществ, таких как улучшенная общая функциональность, и многие специфические функции безопасности в современных IP-сетях. Таким образом, из-за наличия некоторых проблем с безопасностью в сетях IPv6 необходимо предпринимать все возможные шаги для достижения максимального уровня безопасности. IPv6 требует использования протокола IPsec, а также имеет гибкие параметры заголовка расширения. Хотя IPv6 предлагает лучшую безопасность, протокол также создает новые угрозы безопасности. Для улучшения защиты в сетях IPv6 рекомендуется реализовать механизмы безопасности для фильтрации пакетов и обнаружения вторжений. Все ненужные службы должны быть отфильтрованы на брандмауэре. Тем не менее, безопасность протокола IPv6 и сетей IPv6 все еще может быть улучшена, но этот факт не должен быть препятствием для его принятия, использования и дальнейшего развития [4].

Список литературы

1.Контрольная сумма заголовка IPv4. [Электронный ресурс]. Режим доступа: https://ru.qaz.wiki/wiki/IPv4_header_checksum. Дата обращения: 15.12.2020

2. Компьютерные сети Принципы, технологии, протоколы 5-е издание. В. Олифер Н. Олифер.

3. Архитектура безопасности корпоративных сетей. [Электронный ресурс]. Режим доступа: https://www.cnews.ru/reviews/free/oldcom/security/cisco_safe.shtml. Дата обращеня: 18.10.2020.

4. Bradley Huffaker, Luckie Matthew, Kimberly Claffy. [Электронный ресурс]. Режим доступа: https://www.scopus.com/authid/detail.uri?authorId=8434276100. Дата обращения: 19.11.2020.